IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MISSOURI
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF: 121 E. Hunt Avenue, Apartment 303 Warrensburg, Missouri	Case No. 19-SW-00143-JTM

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Brent Yoshikawa, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 121 E. Hunt Avenue, Apartment 303, Warrensburg, Missouri, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with U.S. Immigration and Customs Enforcement, Homeland Security Investigations, and have been since November 16, 2009. In connection with my official duties I investigate criminal violations of federal narcotics and money laundering laws. My training and experience has involved the debriefing of defendants, witnesses, and informants, as well as the collection and analysis of physical, digital, and documentary evidence.

3. I am currently assisting Homeland Security Investigations Special Agent Mark Koch who is investigating a group of individuals around the country who are suspected of committing online identity theft among other crimes. The information in this affidavit includes

facts known personally to me, as well as facts that I have learned from SA Koch and other agents involved in the investigation, as well as review of reports and other documents.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

APPLICABLE LAW OF CRIMES UNDER INVESTIGATION

5. I submit this affidavit in support of an investigation into crimes including, but not limited to, violations of the following statutes.

6. **Wire Fraud (18 U.S.C. 1343):** "Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both."

7. **Attempt and Conspiracy (18 U.S.C. 1349):** "Any person who attempts or conspires to commit any offense under this chapter [including 18 U.S.C. 1343] shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy."

8. **Aggravated Identity Theft (18 U.S.C. § 1028A(a)(1)):** "Whoever, during and in relation to any felony violation enumerated in subsection (c) [including 18 U.S.C. 1343],

knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years."

PROBABLE CAUSE

Background

9. In March of 2018, Homeland Security Investigations ("HSI") Detroit initiated an investigation into a group of individuals who referred to themselves as "The Community." The Community was a loosely organized group of individuals dedicated to online identity theft. Its members specialized in a tactic known as "SIM Hijacking" or "SIM Swapping."

10. This tactic enabled The Community to gain control of a victim's mobile phone number by linking that number to a subscriber identity module ("SIM") card controlled by The Community—resulting in the victim's phone calls and short message service ("SMS") messages being routed to a device controlled by a member of The Community.[1]

11. Upon gaining control of a victim's mobile number, one or more members of The Community would proceed to access an online account of the target by either (1) cracking (or stealing) a password and then requesting a two-factor authentication ("2FA") code be sent to the impersonating device or (2) requesting that a password be reset via a text message. Once an

[1] SIM Hijacking was often facilitated by bribing an employee of a mobile phone provider. Other times, SIM Hijacking was facilitated by "social engineering": a member of The Community would contact a mobile phone provider's customer service—posing as the victim—and request that the victim's phone number be swapped to a SIM card (and thus a mobile device) controlled by The Community.

initial account—typically an email—was compromised, The Community would next seize control of additional accounts by resetting additional passwords linked to the account that they now controlled.

12. During these attacks, one or more members of The Community would appropriate the online identity of the victim, using means of identification including the victim's name, email, and mobile phone number.

13. Members of The Community planned and organized their activities on various online forums and over diverse channels of communication. Broader discussions—such as discussing the manner and means of attacks generally, and networking among The Community's members—typically took place on forums such as "OGUsers" and "Hackforums." Planning and execution of specific attacks, as well as victim selection and recruiting, usually took place via platforms such as Discord, Skype, Signal, Wickr, and Telegram. These services can be accessed by the use of computers, as well as by mobile devices such as phones and tablets.

14. The investigation revealed that a subset of The Community conspired to specialize in the theft of cryptocurrency.[2] These individuals engaged in SIM Hijacking with the goal of gaining control of—and stealing—a target's cryptocurrency.

---

[2] Cryptocurrencies, also known as virtual currencies or digital currencies, are online media of exchange. The most famous is Bitcoin, but many others exist—such as LiteCoin and Ethereum. Like traditional currency, they act as a store of value and can be exchanged for goods and services. They can also be exchanged for dollars. But, unlike "fiat" currencies such as the dollar, they are untethered from the traditional banking system and neither issued nor backed by sovereign states. Their value depends only on the law of supply and demand.

15. The conspirators would conduct research to identify targets for SIM Hijacking that were publicly associated with cryptocurrency, such as investors or promoters. The assumption of the conspirators was that these individuals would have substantial cryptocurrency holdings.

16. If the conspirators were able to successfully hijack a target's phone number, they would use the techniques above to attempt to steal the target's cryptocurrency.

17. In May of 2018, a member of The Community was arrested and began cooperating with law enforcement. Through him, law enforcement gained access to records of online chats between members of The Community. Search warrants were subsequently issued that enabled the review of further online chats between members of The Community.

18. Through review of online chats discussing the planning and execution of cryptocurrency thefts, law enforcement identified victims of The Community. Victims were interviewed and their losses substantiated.

19. Law enforcement also reviewed logs provided from mobile phone providers and online service providers that revealed unauthorized access to victims' phone services as well as email, cloud storage, and cryptocurrency exchange accounts. In numerous instances, law

enforcement was able to identify an IP address or addresses[3] that one or more attackers used to access a victim's online accounts.

20. This investigation has shown that members of The Community have been responsible for thefts of cryptocurrencies in excess of $2,400,000 (as valued at time of theft). The thefts were coordinated and executed via the Internet utilizing several internet platforms, to include Discord,[4] with the intent to hide or disguise the members' true identities. Proceeds from the cryptocurrency thefts were disbursed electronically and in anonymity due to the nature of cryptocurrency transactions.

21. On April 18, 2019, the Grand Jury returned a sealed indictment charging GARRETT ENDICOTT, along with five others, in the Eastern District of Michigan with several counts related to the scheme outlined above, including Conspiracy to Commit Wire Fraud, in violation of 18 U.S.C. § 1349, Wire Fraud, in violation of 18 U.S.C. § 1343, and Aggravated Identity Theft, in violation of 18 U.S.C. § 1028A(a)(1).

---

[3] The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

[4] Discord is a proprietary freeware voice over internet protocol application specializing in text, image, video and audio communication between users in a chat channel.

Garrett Endicott (aka "Halo")

22. Through review of online chats and through interviews, Discord user garrett#5198 and Skype user haloreachfk were identified as belonging to a member of The Community who engaged in SIM swapping and cryptocurrency theft.

23. On or about July 6, 2018, an HSI Detroit Task Force Officer received a search warrant response from Discord that included Discord user garrett#5198, User ID 275079871896748032. This response included chat history, IP addresses, and email address associated to garrett#5198.

24. On or about October 4, 2018, an HSI Detroit Task Force Officer received a search warrant response from Microsoft that included Skype user haloreachfk. This response included chat history, an account report, and a registration report.

25. During the course of the investigation, Discord user garrett#5198 and Skype user haloreachfk were identified as GARRETT ENDICOTT of Kingsville, Missouri.

26. On June 7, 2018, a cooperating individual (CI) who is a member of The Community advised an HSI Detroit analyst that an individual named Garrett was a member of The Community. The CI stated that Garrett's role was providing personally identifiable information (PII) on targets and providing cryptocurrency for SIM swaps. The CI stated that Garrett was a white male that is approximately 18 years old and in college. The CI stated that Garrett teaches karate and has an apartment. The CI stated that Garrett had a Discord account with username "Garrett".

27. On August 1, 2018, the CI identified the user of Skype username haloreachfk as Garrett.

28. From the Discord search warrant response, an HSI Detroit analyst compiled the IP addresses and date ranges for session logins for garrett#5198, which included the following IP addresses belonging to the internet service providers listed below:

IP Address	Count	Start (UTC)	End (UTC)	ISP
76.0.3.210	370	5/22/2018 02:53:32	6/18/2018 01:53:26	Centurylink
97.88.169.146	225	6/2/2018 21:51:23	7/18/2018 06:12:19	Spectrum
76.0.0.140	20	6/20/2018 19:06:37	6/23/2018 20:00:17	Centurylink
153.91.225.103	11	6/4/2018 17:17:48	6/14/2018 21:29:26	University of Central Missouri

29. An HSI Detroit analyst further reviewed the content from chats for garrett#5198. This review identified that Garrett had an email address of gendicott99@gmail.com. This review further identified that garrett#5198 has been involved in The Community since at least March 2017, and enabled trades of accounts that were taken over via SIM swapping. This review also revealed that members of The Community frequently referred to this individual as "Halo."

30. An HSI Detroit analyst also reviewed the attachments for garrett#5198. This review identified images of a white male later identified as GARRETT ENDICOTT.

31. From the Microsoft search warrant response, an HSI Detroit analyst reviewed chats of Skype user haloreachfk. This review identified that haloreachfk used a display name of

"Garrett" and was referred to by others as Garrett. Skype user haloreachfk also provided an email address of gendicott99@gmail.com. Three images sent by Skype user haloreachfk also originated from "C:\Users\Endicott".

32. An HSI Detroit analyst also reviewed the attachments for Skype user haloreachfk. This review identified images of a white male later identified as GARRETT ENDICOTT.

33. On or about August 2, 2018, an HSI Detroit Task Force Officer received a search warrant response from the University of Central Missouri for IP address 153.91.225.103. This response identified the student username attached to the IP address as gfe94960. The individual attached to username gfe94960 was GARRETT F. ENDICOTT, date of birth May 9, 1999, address 1890 NW 260 Road, Kingsville, Missouri. This response included a picture of GARRETT ENDICOTT's student ID photo, which matched images obtained from Discord user garrett#5198 and Skype user haloreachfk.

34. On or about August 16, 2018, an HSI Detroit Task Force Officer received a response from Charter Communications for IP address 97.88.169.146. This response identified the subscriber as GARRETT ENDICOTT with service address **121 E. Hunt Avenue, Apt 303, Warrensburg, Missouri**.

35. On or about September 18, 2018, an HSI Detroit Task Force Officer received a response from CenturyLink for IP addresses 76.0.3.210 and 76.0.0.140. This response identified the subscriber as Bob Endicott, 1890 NW 260th Road, Kingsville, Missouri.

36. Using a commercial database, an HSI Detroit analyst identified that GARRETT ENDICOTT, date of birth May 9, 1999, has resided at 1890 NW 260th Road, Kingsville, Missouri.

37. On or about April 25, 2019, HSI Kansas City Special Agent Ben Gatrost conducted surveillance at **121 E Hunt Avenue, Warrensburg, Missouri**. One of the parking spaces in the parking lot on the south side of the building bears "303" printed on the ground. A red Ford Explorer Sport Trac bearing Missouri registration 3DCU16 was parked in parking space 303. The rear window of the Sport Trac displayed decals printed with "ATA BLACKBELT, GARRETT."

38. Missouri registration 3DCU16 relates to a 2004 Ford registered to Robert L and Debra K Endicott, 1890 NW 260 Road, Kingsville, Missouri 64061.

39. The mail slot for apartment 303 was unlocked and ajar. Inside the mail slot was an envelope from Spire addressed to "Garrett Endicott, **121 E Hunt Avenue Apt 303, Warrensburg, Missouri 64093-2672**".

40. On April 30, 2019, HSI Special Agents Jason Poniatowski and Brent Yoshikawa conducted surveillance at **121 E Hunt Avenue, Warrensburg, Missouri**. A red Ford Sport Trac bearing Missouri registration 3DCU16 was parked in parking space 303 of the apartment building.

121 E. Hunt Avenue, Apartment 303, Warrensburg, Missouri

41. 121 E Hunt Avenue is a three-story brick building located west of Missouri Street and north of E Hunt Avenue in Warrensburg, Missouri. The south side of the building bears a sign stating "Candlelight Apartments" in script. The lobby of 121 E Hunt Avenue can be entered through a glass door on the south side of the building. Above the glass door is a sign on which is printed "121 EAST HUNT". A stairwell in the lobby leads to the third floor. The door to apartment 303 is on the third floor and is the second door from the south side of the building on the west side of the hallway. The door is brown in color on which is mounted a sign with "303" printed in white.

Victim TH

42. On August 14, 2018, an AT&T investigator provided information on IMEIs suspected to be involved in SIM swapping to an HSI Detroit analyst. This information showed that on March 6, 2018, a new SIM card was activated for phone number XXX-XXX-7068 (TH's mobile phone number) on IMEI 354450068482982. An iPhone with IMEI 354450068482982 was seized from a known member of The Community in or around March 2018.

43. On or about March 6, 2018, ENDICOTT, as Skype user haloreachfk, participated in a Discord chat furthering a scheme to defraud victim TH of his cryptocurrency. ENDICOTT and others conspired to use TH's identity to seize control of multiple online accounts—including an email account, a Twitter account, cryptocurrency exchange accounts, and a cryptocurrency wallet.

44. ENDICOTT's role in The Community was to research victims and to provide personally identifiable information (PII) associated with victims to facilitate the theft of their identities.

45. From reviewing the Skype chat history and other investigative means, it had been determined that on or about March 6, 2018, ENDICOTT and others conspired to seize control of TH's cryptocurrency wallet and steal approximately $4,929.37.

46. On September 26, 2018, an HSI Detroit Task Force Officer and an HSI Detroit analyst called victim TH regarding his SIM hijacking and subsequent theft of cryptocurrency. TH stated that he had several accounts compromised included his Twitter, Hotmail, Bittrex, and Binance. TH also stated that his Exodus wallet was compromised, and that he lost approximately $5,000 in Litecoin.

47. On September 26, 2018, TH emailed HSI Detroit regarding the theft of his cryptocurrency. This included a screenshot of a transaction in the amount of 25.01819531 LTC sent to Litecoin address XXXXf9XjW. An HSI Detroit analyst verified this transaction.

48. An HSI Detroit analyst conducted analysis of the Litecoin blockchain, which identified that the Litecoin was split into multiple portions within three hours of the initial transfer. An HSI Detroit analyst identified that 5.10529207 LTC of the initial 25.01819531 LTC was seized from a known member of the Community on June 8, 2018.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

49. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

50. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being

used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

51. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion.

    i. In my training and experience, information stored within a computer or storage media (e.g., registry information, personal communications, personal images and movies, transactional information, records of session

times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

ii. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner.

iii. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.

iv. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on

a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user.

v. Information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain unauthorized access to a victim's online accounts over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this

type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

52. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the

warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

53. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

54. Because several people may share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

SEARCHES FOR EVIDENCE PERTAINING TO CRYPTOCURRENCY

55. As described *supra*, this investigation involves the theft of cryptocurrency.

56. Cryptocurrency is stored in "wallets" both online and offline. In order to access and send the cryptocurrency stored in these wallets, the owner of the cryptocurrency must have access to both the wallet address, also known as a public key, and the private key. Both the wallet address and private key are lengthy, facially unintelligible, strings of letters and/or numbers.

57. Recovery seeds are a series of random words which store the information needed to recover all of the public key-private key pairs of a cryptocurrency wallet. Recovery seeds allow an owner of virtual currency to access his/her wallet from any electronic device.

58. Cryptocurrency can be—but is not necessarily—stored in so-called "hardware wallets," physical devices produced by companies such as SatoshiLabs or Ledger that contain the wallet addresses and private keys necessary to access and transfer cryptocurrency. A user of such

a device may store the password or passwords necessary to access such an account on a phone, computer, or other electronic storage device.

59. Cryptocurrency can be—but is not necessarily—stored in online wallets, some of which are controlled by the operators of online cryptocurrency exchanges. In the case of a user of an online wallet, electronic devices such as phones or computers would contain records pertaining to its access. A user may also store the password or passwords necessary to access such an account on a phone, computer, or other electronic storage device.

60. Some cryptocurrency owners write their private keys, wallet addresses, recovery seeds and/or passwords down or print them out on paper and hide them in various places such as picture frames, safes, desks, etc., as backup so that they do not lose access to their wallets.

61. Some cryptocurrency owners store their private keys, wallet addresses, recovery seeds, and/or passwords on their computers, cell phones, or other electronic storage devices. On an electronic storage device, such keys, addresses and passwords can be stored in any form and—like other valuable electronic information—are sometimes concealed or encrypted. Concealment of electronic files can take place by many means, including but not limited to renaming files, changing file extensions, hiding files in unusual places (such as among word

processing documents or photographs), or using various publically available programs to encrypt or hide them.

62. Some cryptocurrency owners will take pictures of their private keys, wallet addresses, recovery seeds, and/or passwords and store them electronically. Such photographs may be concealed or encrypted as described in the preceding paragraph.

63. In my training and experience, cryptocurrency users closely control access to cryptocurrency. The information used to access and transfer cryptocurrency—as well as the electronic devices used to do so—will typically be located on the person of a cryptocurrency user, at their home, and/or at another secure location readily accessible to the user.

64. In my training and experience, users of cryptocurrencies—especially those that have stolen it—often convert one cryptocurrency into another. For those that have stolen cryptocurrency, these transfers are often done to attempt to conceal stolen funds and make them more difficult to trace.

65. There are a myriad of cryptocurrencies, including but not limited to Bitcoin, Ethereum, Ripple (XRP), Bitcoin Cash, Litecoin, EOS, Binance Coin, Stellar, Cardano, Monero, Zcash, Dash, Dogecoin, and Verge.

CONCLUSION

66. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

REQUEST FOR SEALING

67. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

Brent Yoshikawa
Special Agent
U.S. Immigration and Customs Enforcement

Subscribed and sworn to before me
On May 3, 2019

Honorable John T. Maughmer
United States Magistrate Judge
Western District of Missouri.